## Amendments to the Claims

Please amend claims to be as follows.

- 1. (currently amended) A method for secure remote mirroring of network traffic, the method comprising:
  - receiving a data packet to be remotely mirrored by an entry device pre-configured with a mirroring destination address to which to mirror the data packet;
  - forwarding the data packet in unencrypted form towards an original destination address indicated in the data packet;
  - encrypting a copy of the data packet to form an encrypted packet;
  - incrementing an identifier for indicating a position of the [[data]] encrypted packet within an order of packets received by the entry device for remote mirroring;
  - generating and adding a header to encapsulate the encrypted data packet, wherein the header includes the <u>mirroring</u> destination address and said identifier; and
  - forwarding the encapsulated encrypted packet to an exit device associated with the mirroring destination address.
- (currently amended) The method of claim 1, wherein the <u>mirroring</u> destination address comprises an Internet protocol (IP) destination address, wherein the header comprises an IP header; and wherein the encapsulated encrypted packet comprises an IP-encapsulated encrypted packet.
- (currently amended) The method of claim 1, wherein the mirroring destination
  address comprises a media access control (MAC) destination address, and wherein
  the header comprises a MAC header, and wherein the encapsulated encrypted packet
  comprises a MAC-encapsulated encrypted packet.
- 4. (original) The method of claim 2, further comprising:

Page 3 of 13 Atty. Docket No. 200314975-1

determining a media access control (MAC) address associated with the destination IP address;

generating and adding a MAC header to the IP-encapsulated packet to form a MAC data frame, wherein the MAC header includes the MAC address in a destination field; and

transmitting the MAC data frame to communicate the IP-encapsulated packet across a layer 2 domain.

- 5. (original) The method of claim 4, wherein determining the MAC address comprises: determining if a mapping of the destination IP address to the MAC address is stored in an address resolution protocol (ARP) cache; if so, then retrieving the MAC address from the ARP cache; and if not, then broadcasting an ARP request with the destination IP address and receiving an ARP reply with the MAC address.
- 6. (currently amended) The method of claim 4, wherein the IP-encapsulated encrypted packet is communicated across multiple intermediate layer 2 domains.
- 7. (previously presented) The method of claim 1, further comprising: receiving the encapsulated encrypted packet by the exit device; removing the header to de-encapsulate the encrypted packet; and decrypting the encrypted packet to re-generate the data packet; and using said identifier to determine the position of the data packet within the order of packets received by the entry device for remote mirroring.
- 8. (original) The method of claim 7, wherein the encrypting and decrypting is performed under a public-private key encryption scheme.

- 9. (original) The method of claim 8, wherein the encrypting is performed using a public key of a destination device, and wherein the decrypting is performed using a corresponding private key of the destination device.
- 10. (original) The method of claim 1, further comprising: configuring the entry device in a best effort mirroring mode to reduce head-ofline blocking.
- 11. (original) The method of claim 1, further comprising:
  configuring the entry device in a lossless mirroring mode to assure completeness
  of mirrored traffic.
- 12. (original) The method of claim 1, further comprising:
  truncating the data packet to reduce a size of the data packet prior to encryption
  thereof.
- 13. (original) The method of claim 1, further comprising:

  compressing at least a portion of the data packet to reduce a size of the data

  packet prior to encryption thereof.
- 14. (currently amended) A networking device comprising:
  - a plurality of ports for receiving and transmitting packets therefrom, wherein the packets are transmitted based on original destination addresses indicated therein;
  - a secure remote mirroring engine configured to detect packets from a specified mirror source, to use an incrementing identifier to indicate an order of the detected packets, to encrypt copies of the detected packets, to encapsulate the encrypted packets using a header which includes said identifier, and to forward the encapsulated encrypted packets to a pre-configured destination address by way of at least one of the ports; and

Page 5 of 13 Atty. Docket No. 200314975-1

Amendment and Response to Final Office Action Application No. 10/813,730

an encryption module configured to be utilized by the remote mirroring engine during encryption of the detected packets.

- 15. (currently amended) The networking device of claim 14, wherein the <u>preconfigured</u> destination <u>address</u> comprises an Internet protocol (IP) destination address.
- 16. (currently amended) The networking device of claim 15, wherein the remote mirroring engine encrypts the <u>copies of the detected</u> packets using a public key of a public-private key pair.
- 17. (currently amended) A system for secure remote mirroring of network traffic, the system comprising:
  - a mirror entry device including a secure mirroring engine configured to detect packets from a specified mirror source, to use an incrementing identifier to indicate an order of the detected packets from the specified mirror source, to encrypt copies of the detected packets using an encryption module, encapsulate the encrypted packets using a header which includes said identifier, and to forward the encapsulated encrypted packets to a preconfigured destination by way of at least one of the ports, wherein the pre-configured destination is distinct from original destinations indicated in the detected packets, and wherein the detected packets are forwarded in unencrypted form towards the original destinations; and
  - a mirror exit device including a secure mirroring receiver configured to detect and decapsulate the encapsulated encrypted packets from the mirror entry device and to re-order and decrypt the encrypted packets.
- 18. (original) The system of claim 17, wherein the encrypting and decrypting is performed under a public-private key encryption scheme.

Page 6 of 13 Atty. Docket No. 200314975-1

Amendment and Response to Final Office Action Application No. 10/813,730

- 19. (original) The system of claim 18, wherein the encrypting is performed using a public key of a destination device, and wherein the decrypting is performed using a corresponding private key of the destination device.
- 20. (currently amended) A system for secure remote mirroring of network traffic, the system comprising a mirror entry device including means to encrypt copies of the detected packets using an encryption module and to encapsulate the encrypted packets using a header which includes an incrementing identifier and a preconfigured destination address associated with a mirror exit device, wherein the preconfigured destination is distinct from original destinations indicated in the detected packets, and wherein the detected packets are forwarded in unencrypted form towards the original destinations; and [[a]] the mirror exit device including means to decapsulate the encapsulated encrypted packets from the mirror entry device and to re-order and decrypt the encrypted packets.
- 21. (currently amended) A method for secure remote mirroring of network traffic, the method comprising:
  - remotely configuring an entry device with an encryption key and mirroring destination address;
  - remotely configuring an exit device at the <u>mirroring</u> destination address with a decryption key;

receiving a data packet to be mirrored by the entry device;

- incrementing an identifier to indicate a position of the data packet within an order of packets mirrored by the entry device;
- encrypting <u>a copy of</u> the data packet using the encryption key to form an encrypted packet;
- generating and adding a header to encapsulate the encrypted data packet, wherein the header includes the <u>mirroring</u> destination address and said identifier;

  [[and]]
- forwarding the data packet in unencrypted form to an original destination address indicated in the data packet; and

forwarding the encapsulated encrypted packet to the mirroring destination address of the exit device.

- 22. (original) The method of claim 21, wherein the remote configuration is performed by way of SNMP.
- 23. (original) The method of claim 21, wherein the remote configuration is performed by way of a secure remote protocol.